UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Carla Tracy on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. ELEKTA, INC., Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Carla Tracy ("Plaintiff"), brings this Class Action Complaint, on behalf of herself and all others similarly situated (the "Nationwide Class" and the "Illinois Subclass"), against Defendant Elekta, Inc. ("Elekta" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge.

NATURE OF CASE

1. Plaintiff brings this class action against Defendant Elekta for its failure to properly secure and safeguard highly-valuable, protected personally identifiable information ("PII"), and protected health information ("PHI"), including without limitations, patient names, dates of birth, Social Security numbers, health insurance information, medical record numbers, and clinical information related to cancer treatment, such as medical histories, physician names, dates of service, treatment plans.

2. Elekta maintains a first-generation cloud-based data storage system that serves cancer healthcare providers. Elekta experienced a ransomware attack and subsequent data breach between April 2, 2021 and April 20, 2021, the result of which allowed hackers to gain unauthorized access to Elekta's cloud-based radiology software ("Data Breach").

3. As a result of the Data Breach, Elekta temporarily was forced to take its software offline until the security vulnerabilities could be identified and addressed, which in turn prevented or delayed treatment for many cancer patients across the United States.

4. Ironically, while Elekta offers data analytic solutions to its clients, it failed to secure its own systems from cybercriminals. In fact, Elekta engaged in a forensic investigation and on April 28, 2021 cautioned that "Elekta must conclude that all data within Elekta's first-generation cloud system was compromised."

5. Due to Elekta's inadequate data security and failure to comply with federal, state, and industry data privacy standards, an unauthorized third party used compromised credentials to gain access to Elekta's digital environment. Thereafter, the unauthorized third-party gained access to, and then exfiltrated, the files and records of various businesses customers of Elekta, including Northwestern Memorial HealthCare, Renown Health, St. Charles Health System, Carle Health, Cancer Centers of Southwest Oklahoma, LLC, Lifespan, Southcoast Health, and Yale New Haven Health.

6. Due to Elekta's negligence and inadequate data security, Plaintiff and Class members have suffered actual harm and are subject to an increased risk of identity theft. Plaintiff's and Class members' PII/PHI have been compromised and they must now undertake additional security measures to minimize the risk of identity theft.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

8. This Court has jurisdiction over Defendant because Elekta maintains its United States principal place of business at 400 Perimeter Center Terrace, Suite 50, Dunwoody, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Georgia to many businesses nationwide.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Elekta's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

10. Plaintiff Carla Tracy is a resident of Dekalb, Illinois and brings this lawsuit on behalf of herself and all others similarly situated. Plaintiff received a notice, dated June 25, 2021, informing her that her PII/PHI had been compromised by a cyberattack and confirmed that data involved in the cyberattack contained patient data stolen from Northwestern Memorial HealthCare because its business associate, Defendant, experienced the Data Breach.

11. Defendant is a Swedish radiation therapy, radiosurgery and related equipment and data services provider incorporated and doing business in Dunwoody, Georgia.

FACTUAL BACKGROUND

12. Elekta was founded in 1972 in Stockholm, Sweden and is currently listed on the

Nordic Exchange under the ticker "EKTAb" even though nearly half of the company's sales are in the United States. With approximately 4,300 employees worldwide, Elekta generates approximately $1.6 billion dollars in annual sales globally with approximately $365 million annually in the United States.

13. Twenty-five percent (25%) of Elekta's annual revenue is derived from its software services.[1] Elekta's software service business provides a "large stream of recurring revenues based on long-term service contracts" with its healthcare customers.

14. Elekta describes itself as "a global leader in radiotherapy solutions to fight cancer and neurological diseases." "We have a broad offering of advanced solutions for delivering the most efficient radiotherapy treatments."[2]

15. Recognizing that the treatment of cancer is "complex and data driven," Elekta has seized on the big data and artificial intelligence healthcare market to increase its revenues. Tailoring its oncology software to capture and leverage patient data to allow healthcare provider clients access to relevant data aimed at automating healthcare processes and driving business decisions.

16. Elekta captures and stores the patient PII and PHI of its radiotherapy clients, asserting that it attempts to analyze this data and improve clinical outcomes, productivity and ultimately increased financial performance of the healthcare provider.

17. Recognizing the highly competitive and regulated healthcare industry in the U.S., Elekta claims to maintain "[s]ound practices for risk management" which "are an essential element of our culture, corporate governance, strategy development, and operational and financial

[1] https://www.elekta.com/investors/fileadmin/reports/annual-reports/elekta-annual-report-2020-21-en.pdf at pg. 18 (last visited July 14, 2021).
[2] *Id.* at Content.

management."[3] In turn, Elekta has established an Enterprise Risk Management (ERM) framework to provide guidance on governance, risk management and internal controls.[4]

18. Despite an identified operational risk that mentions that there needs to be an "appropriate measure[] to protect the data against damage,"[5] and further notes that there is "an increasing threat of material cyber and information security attacks targeting healthcare data,"[6] Defendant has failed to adequately secure Plaintiff's and Class members' PII and PHI.

19. As detailed more fully below, Elekta failed to safely and securely store the PII and PHI entrusted to it and failed to prevent it from being compromised during the Data Breach.

A. The Data Breach

20. As a major component of its oncology and neuroscience business, Elekta maintains large volumes of its clients' PII and PHI. As such, Elekta is well aware of the value of healthcare patient data and highly sought by cybercriminals.

21. Elekta sells itself as able to "[p]rotect your data" with improved data security and AI along with multi-layer threat protection, better data organization leveraging modular infrastructure and disk encryption at rest.[7] Elekta "ensures that safeguarding your clinical data is our highest priority."

22. Yet, while its customers reasonably believed their patients' data was safe within Elekta's confines, in April 2021, Elekta allowed cyber criminals to infiltrate Elekta's data infrastructure's security walls.

23. In late April 2021, Elekta was the subject of a ransomware attack that targeted its

---

[3] *Id*. at 34.
[4] *Id.*
[5] *Id*. at 35.
[6] *Id.* at 98.
[7] https://www.elekta.com/software-solutions/cloud-solutions/ (last visited July 14, 2021)

cloud-based systems, maintaining oncology and radiology data, including that of Plaintiff and Class members. Included in the ransomware attack was the PII andPHI provided to Elekta by certain of its oncology and radiology healthcare clients. Shortly thereafter, Elekta began emailing its clients that it was taking action to immediately cut off the cyberattackers by temporarily taking its systems offline and cancelling or rescheduling radiation treatment appointments for cancer patients.

24. In late May 2021, Elekta began notifying its healthcare clients that their clinical information containing the PII and PHI of patients may have been compromised in the ransomware Data Breach.

25. Elekta's healthcare clients began notifying their patients, including Plaintiff and Class members. For example, in June 2021, Northwestern Memorial HealthCare notified approximately 201,197 patients that "an unauthorized individual gained access to [Elekta's] systems between April 2, 2021 and April 20, 2021 and, during that time, acquired a copy of the database that stores some oncology patient information."[8] Additionally, on or about June 25, 2021, Renown Health notified approximately 65,181 patients that "[w]e are writing to inform you of a recent data security incident that involved our business associate, Elekta, Inc. ('Elekta')."[9]

26. Additional data breach notifications went out to other Elekta clients such as Cancer Centers of Southwest Oklahoma, Carle Health, Lifespan, Charles Health System, Yale New Haven Health, Emory Healthcare and Southcoast Health. In total, approximately 42 healthcare systems are believed to have been affected by the Data Breach that happened on Elekta's watch.

27. The various data breach notices have indicated the stolen PII and PHI included full names, Social Security numbers, addresses, dates of birth, height, weight, medical diagnoses,

[8] https://www.nm.org/patients-and-visitors/notice-of-privacy-incident (last visited July 14, 2021)
[9] file:///C:/Users/nprosser/Downloads/Elekta_Media-Notice%20(1).pdf (last visited July 14, 2021)

medical treatment details, appointment confirmations, and other personal and protected information. Specifically, Plaintiff's notice indicated the data involved in the Data Breach "may have included patient names, dates of birth, Social Security numbers, health insurance information, medical record numbers, and clinical information related to cancer treatment, such as medical histories, physician names, dates of service, treatment plans, diagnoses, and/or prescription information."

28. Soon after the breach notification, an Elekta representative explained:

> Elekta was subjected to a series of cyberattacks which affected a subset of U.S.-based customers on our first-generation cloud system. On April 20, to contain and mitigate the attacks, Elekta proactively took down its first-generation cloud system in the United States. An investigation is being conducted, and any affected customer(s) will be contacted and fully briefed through the appropriate channels and in accordance with any legal requirements.[10]

29. As a result of the Data Breach, many cancer patients across the United States had their cancer treatment delayed or disrupted when Elekta decided to temporarily take its system offline to protect any further exfiltration of patient and customer's information.

B. Data Breaches Lead to Identity Theft and Cognizable Injuries.

30. The personal, health, and financial information of consumers, such as Plaintiff's and Class members', is valuable and has been commoditized in recent years.

31. Elekta is well aware that the PII and PHI it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

32. Elekta knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security were breached. Elekta failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

[10] https://compliancy-group.com/healthcare-vendor-ransomware-attack-170-health-systems-hit/ (last visited July 14, 2021)

33. PII and PHI are valuable commodities to identity thieves, particularly when it is aggregated in large numbers when multiple types of information for a single user are combined. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical or financial fraud.

34. The ramifications of Defendant's failure to keep Plaintiff's and Class members' PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

35. According to industry experts, one out of four data breach notification recipients becomes a victim of identity fraud.

36. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

37. Once PII and PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

38. According to the FBI's Internet Crime Complaint Center (IC3) 2020 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $4.1 billion in losses to individuals and business victims.[11]

39. In 2020 as the COVID-19 global pandemic permeated all aspects of life, cyber

[11] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited July 14, 2021)

fraudsters took the opportunity to exploit the pandemic and targeted both businesses and individuals.[12] As healthcare systems experienced an unprecedented challenge of grappling with the varying components and effects of COVID-19, a major ramification also was exploited by the increase in data breaches to patient data.[13]

40. In addition to the exposure directly related to data breaches involving PII and PHI effectuated through the healthcare system, victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opening accounts or misuse of existing accounts.

41. Data breaches facilitate identity theft as hackers obtain consumers' PII and PHI, thereafter using it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII and PHI to others who do the same.

42. Moreover, in light of the current COVID-19 pandemic, Plaintiff's sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

43. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

44. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, many victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent

[12] *Id.*
[13] https://www.prnewswire.com/news-releases/health-data-breaches-skyrocket-during-covid-19-pandemic-301247097.html (last visited July 14, 2021)

information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

45. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII and PHI. To protect themselves, Plaintiff and Class members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

46. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

47. Recognizing the high value consumers place on their PII and PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[14]

48. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of same. Research shows how much consumers value their data privacy, and the amount is considerable.

[14] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed July 14, 2021)

49. By virtue of the Data Breach here and unauthorized release and disclosure of the PII and PHI of Plaintiff and the Class, Defendant has deprived Plaintiff and Class members of the substantial value of their PII and PHI, to which they are entitled. As previously alleged, Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

50. According to the FTC, unauthorized PII and PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[15]

51. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

52. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

53. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class members' PII and PHI, Plaintiff and all Class members have suffered, and will continue to

[15] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last accessed July 14, 2021)

suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) out-of-pocket expenses for securing identity theft protection and other similar necessary services.

C. FTC Guidelines Prohibit Unfair or Deceptive Acts

54. Elekta is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

56. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[17]

57. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used

[16] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 14, 2021)
[17] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf (last visited May 21, 2021)

on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Elekta failed to properly implement basic data security practices. Elekta's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

60. Elekta was at all times fully aware of its obligations to protect the PII and PHI of consumers because of its business model of collecting PII and PHI and storing such information for analysis and for pecuniary gain. Elekta was also aware of the significant repercussions that would result from its failure to do so.

CLASS DEFINITION AND ALLEGATIONS

61. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

The Nationwide Class:

> All persons residing in the United States who had their PII and/or PHI hosted by Elekta compromised as a result of the Data Breach.

The Illinois Class:

> All persons residing in the State of Illinois who had their PII and/or

[18] *Id.*

PHI hosted by Elekta compromised as a result of the Data Breach.

Excluded from the Class and Subclass are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries; (ii) the Judge presiding over this action; and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches.

62. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

63. The members of the Class and Subclass are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes over 200,000 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

64. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their PII and PHI;

d. whether Defendant breached its duty to protect the PII and PHI of Plaintiff and the other Class members;

e. whether Defendant knew or should have known about the inadequacies of their data protection, storage, and security;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and the other Class members' PII and PHI from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's computer systems and digital storage environment;

h. whether Defendant had the proper computer systems to safeguard and protect Plaintiff's and the other Class members' PII and PHI from unauthorized theft, release or disclosure;

i. whether Defendant breached its promise to keep Plaintiff's and the Class members' PII and PHI safe and to follow federal data security protocols;

j. whether Defendant's conduct was the proximate cause of Plaintiff's and the other Class members' injuries;

k. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

l. whether Plaintiff and the other Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;

m. whether Plaintiff and the other Class members are entitled to recover actual damages and/or statutory damages; and

n. whether Plaintiff and the other Class members are entitled to other appropriate remedies, including injunctive relief.

65. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the other Class members. Individual questions, if any, pale by

comparison, in both quality and quantity, to the numerous common questions that dominate this action.

66. Plaintiff's claims are typical of the claims of the members of the Class and Subclass. All Class members were subject to the Data Breach and had their PII and PHI accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in a similar manner.

67. Plaintiff will fairly and adequately protect the interests of the members of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

68. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

69. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

70. Upon gaining access to the PII and PHI of Plaintiff and members of the Class, Defendant owed to Plaintiff and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII and PHI of Plaintiff and the Class. Defendant further owed to Plaintiff and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

71. Defendant owed this duty to Plaintiff and the other Class members because Plaintiff and the other Class members compose a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with Plaintiff's and the other Class members' PII and PHI when obtaining and using Defendant's services. To facilitate these services, Defendant used, handled, gathered, and stored the PII and PHI of Plaintiff and the other Class members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII and PHI that Defendant actively solicited from clients who entrusted Defendant with Plaintiff's and the other Class members' data. As such, Defendant knew a breach of its systems would cause damage to its

clients and Plaintiff and the other Class members. Thus, Defendant had a duty to act reasonably in protecting the PII and PHI of its healthcare clients' patients.

72. Defendant breached its duty to Plaintiff and the other Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII and PHI of Plaintiff and the other Class members.

73. Defendant also breached its duty to timely and accurately disclose to the clients, Plaintiff and the other Class members, that their PII/PHI had been or was reasonably believed to have been improperly accessed or stolen.

74. Defendant's negligence in failing to exercise reasonable care in protecting the PII/PHI of Plaintiff and the other Class members is further evidenced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

75. The injuries to Plaintiff and the other Class members were reasonably foreseeable to Defendant because laws and statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the other Class members' PII and PHI.

76. The injuries to Plaintiff and the other Class members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII and PHI were inadequately secured and exposed consumer PII and PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiff and the other Class members.

77. The injuries to Plaintiff and the other Class members also were reasonably foreseeable because Defendant, all persons in the healthcare and healthcare support industries, and

are large portion of the general public are aware of the high and ever increasing incidence of cyberattacks perpetrated against healthcare providers, including the upward spike of cyberattacks targeted against companies in the healthcare industry during the COVID pandemic.

78. Defendant's failure to take reasonable steps to protect the PII and PHI of Plaintiff and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiff's and the other Class members' PII and PHI. This ease of access allowed thieves to steal PII and PHI of Plaintiff and the other Class members, which could lead to dissemination in black markets.

79. As a direct proximate result of Defendant's conduct, Plaintiff and the other Class members have suffered theft of their PII and PHI. Defendant allowed thieves access to Class members' PII and PHI, thereby decreasing the security of Class members' financial and health accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Plaintiff and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

80. Defendant's conduct warrants moral blame because Defendant actively solicited its services to its clients, wherein it used, handled and stored the PII and PHI of Plaintiff and the other Class members without disclosing that its security was inadequate and unable to protect the PII and PHI of Plaintiff and the other Class members. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing larger IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

81. As a direct and proximate result of Elekta's negligence, Plaintiff and Class members

have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, and punitive damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

82. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Elekta for failing to use reasonable measures to protect PII/PHI. Various FTC publications and orders also form the basis of Elekta's duty.

84. Elekta violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Elekta's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of a data breach.

85. Elekta's violation of Section 5 of the FTC Act constitutes negligence *per se*.

86. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

87. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

88. As a direct and proximate result of Elekta's negligence, Plaintiff and Class members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

89. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

90. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

91. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and PHI, including whether Elekta is currently maintaining data security measures adequate to protect Plaintiff's and Class members from further data breaches that compromise their PII/PHI. Plaintiff alleges that Elekta's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

92. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Elekta owes a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act; and

b. Elekta continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

93. This Court also should issue corresponding prospective injunctive relief requiring Elekta to employ adequate security protocols consistent with law and industry standards to protect consumers' PII and PHI.

94. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Elekta. The risk of another such breach is real, immediate, and substantial. If another breach at Elekta occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

95. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Elekta if an injunction is issued. Plaintiff and Class members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Elekta of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Elekta has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Elekta, thus eliminating the additional injuries that would result to Plaintiff and consumers whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as a representative of the Class and Plaintiff's

attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded: and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Carla Tracy, on behalf of herself individually and the putative Class, demands a trial by jury on all claims so triable.

Respectfully Submitted,

THE FINLEY FIRM, P.C.

Dated: July 16, 2021

/s/ MaryBeth V. Gibson

MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Fax: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Gary M. Klinger*
MASON LIETZ & KLINGER, LLP
227 W. Monroe Street, Ste. 2100
Chicago, IL 60606

Tel: (202) 975-0477
gklinger@masonllp.com

Bryan L. Bleichner*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Ste. 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Nathan D. Prosser*
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

ATTORNEYS FOR PLAINTIFF

**Pro Hac Vice Forthcoming*